COSMOS
Navigate the Compliance Universe

HCCA Compliance 101, Fifth Edition
Chapter 10. Privacy and Security

By Darrell W. Contreras

The privacy and security of patient information is a critical component of any organization's compliance program. In addition to the legal and regulatory obligations to protect patient information, the past few years have demonstrated the value of patient information to those who attempt to obtain it illegally. In the years following the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the biggest breach concerns were employees inappropriately viewing and disclosing patient information and large-scale disclosures resulting from a lack of protective safeguards for data at rest on unencrypted devices, for example. However, although advances in technology have made it easier to secure data, those technological advances have also increased the threat of data breach from external intrusion by hackers.

For compliance professionals working in healthcare settings, it is critical to have a solid understanding of the requirements and exceptions of the HIPAA Privacy and Security rules. Although there are other privacy laws that can have an impact on healthcare organizations, the HIPAA Privacy and Security rules apply to virtually all healthcare entities.For a summary of other healthcare privacy laws, see HCCA's *Health Care Privacy Compliance Handbook, Third Edition*.[1]

HIPAA Overview

HIPAA passed in 1996 as the Health Insurance Portability and Accountability Act. The intent of the legislation was to reduce the administrative costs of healthcare. The HIPAA legislation was intended to address several areas of the healthcare system, including: the availability, portability, and renewability of health insurance; fraud and abuse laws; tax laws; the administrative costs in healthcare data and payment transmissions; and the application and enforcement provisions of group health plan regulations. HIPAA included provisions to provide for the "portability" of insurance plans; address fraud, waste, and abuse in the healthcare system; and facilitate the electronic submission of claims and payment through the transaction and code sets provision. But the most recognizable aspect of HIPAA is the protections it created for protected health information (PHI) created or maintained by covered entities. Specifically, HIPAA governs the use and disclosure of PHI by covered entities directly and their business associates (including subcontractors of business associates) indirectly. If the organization in question does not fit the definition of a covered entity, the regulations do not apply.

At the time of its enactment, Congress recognized approximately 24 cents of every dollar spent on healthcare was being spent on administrative costs and not on what was most important: the provision of healthcare to individuals. One reason for the high administrative costs was the use of proprietary technology transactions between those who provided healthcare and those who paid for healthcare. Congress identified more than 400 proprietary methods for transmitting information between providers and payers. The solution was to mandate standard formats for transactions and code sets to be used in healthcare.

The standardization of electronic health information brought with it an increased concern that health information could be more readily acquired and used for inappropriate purposes. As a result, Congress added provisions to the statute that paved the way for what are now commonly referred to as the HIPAA Privacy and Security rules.

The Administrative Simplification Section of Title II is the section of HIPAA that required the development of uniform transaction standards for content and transmission of the data, requirements for a single National Provider Identification number for all healthcare providers, as well as the Privacy and Security rules to protect health information.

HIPAA Terms and Acronyms

Most healthcare providers experience the impact of the Administrative Simplification Section of HIPAA in virtually every aspect of their work. Any piece of legislation passed by Congress will result in new terms and acronyms. HIPAA is no exception. Key terms are included in the glossary. Reviewing these terms may be necessary to better understand concepts discussed in this chapter.

Congress did not come to agreement on a legislative Privacy or Security standard and therefore, the implementation of the Privacy and Security rules were delegated to the U.S. Department of Health & Human Services. The final Privacy Rule was released originally in October 2000 and had a final effective date of April 14, 2003. The final Security Rule was published later and became effective on April 21, 2005.

The Privacy Rule has two essential approaches to protecting the privacy of health information. First, the rule assigns rights to individual patients to provide them with some control over their health information. Secondly, it provides standards for the ways that healthcare providers, health plans, and healthcare clearinghouses (collectively referred to as "covered entities") are permitted to use and disclose health information.

The HIPAA Privacy and Security rules also include certain administrative requirements such as the requirement for a Privacy Officer; implementation of safeguards to protect the confidentiality, integrity, and availability of information; and training and education requirements. The focus of this chapter is the rights of the individual to access personal information, and the rules for providers and health plans to use and disclose health information.

Preemption of HIPAA

HIPAA is a national regulation, and generally, if a federal statute states that it preempts or overrides state laws on a particular issue, then the federal law is the law that must be followed. The HIPAA statute has a modified preemption clause and is often termed a "floor," in that it provides a national standard for the protection of health information that can be preempted by state laws in certain limited respects.

As a general rule, HIPAA will apply. In some states there may be specific aspects of state law that can be more protective of the information or can provide patients with greater access or other rights to control their information, and thus would supersede the federal Privacy Rule. Although many state laws have focused on data privacy protections in a context that is much broader than just healthcare, the scope of those laws can include data created, used, and maintained by healthcare organizations that operate within those states. For that reason, it is important for compliance professionals to keep apprised of changes to state laws that impact data privacy—and assess the extent to which those laws apply to their organizations.

Organizations that do business in one or more states must be aware of and familiar with the state privacy laws that may provide greater protections than HIPAA. Your state department of health and legal counsel may be resources that can assist with this effort. Regardless of how the information is obtained, compliance professionals must be vigilant in monitoring changes to state laws that involve the protection of patient data and

information.

HITECH Act and the Omnibus Rule

Since the HIPAA rules went into effect, additional laws have modified some aspects of the Privacy and Security rules. The Health Information Technology for Economic and Clinical Health (HITECH) Act passed in February 2009 as part of the American Recovery and Reinvestment Act (ARRA). HITECH was designed to promote widespread adoption and standardization of electronic health records. The act modified HIPAA Privacy and Security rules and represented the first significant changes to the rules since the original effective dates. HITECH included notification requirements for breaches of unsecured protected health information, increased the potential civil monetary penalties for HIPAA violations, and strengthened certain privacy rights. In addition, HITECH extended the obligations of covered entities to protect the privacy and security of PHI to business associates of covered entities.

On January 25, 2013, HHS published the final rule to implement the statutory amendments under HITECH and to implement Section 105 of Title I of the Genetic Information Nondiscrimination Act (GINA). This rule became known as the "Omnibus Rule" and went into effect March 26, 2013, but covered entities were given until September 23, 2013, to comply with its requirements.

The Omnibus Rule made several modifications to the privacy practices that covered entities must implement, including:

- Expanding to include subcontractors of business associates and increasing the obligations of business associates of covered entities to protect the privacy and security of PHI
- Modifying the standard for a reportable privacy breach and specification of the assessment criteria
- Excluding from the definition of marketing any treatment communications about health-related products or services by a healthcare provider to an individual, provided that certain opt-out conditions are included
- Prohibiting the sale of PHI without an individual's authorization
- Requiring covered entities to provide an "opt out" option for fundraising activities
- Requiring that additional, specific language be included in the Notice of Privacy Practices
- Supplementing individual rights to access PHI in electronic records
- Permitting payments for PHI for research purposes provided that the payment is limited to "a reasonable cost-based fee to cover the cost to prepare and transmit" the PHI for research purposes
- Excluding HIPAA privacy and security protections for PHI of individuals who have been deceased for more than 50 years
- Expanding the exception for disclosures for public health to include disclosures of proof of immunization by covered entities to schools in states that have school entry or similar laws
- Putting a restriction on information provided to health plans for healthcare that an individual has paid in full out of pocket

HIPAA Standard Transaction and Code Sets

HIPAA's Administrative Simplification Section of Title II established standard transaction and code sets. The technical make-up of a standard transaction is beyond the introductory intent of this chapter. However, an introduction to the standard transaction and code sets is appropriate.

The **standard transaction sets** under HIPAA are:

- 837: Claim/encounter submission
- 834: Enrollment and disenrollment
- 270, 271: Eligibility
- 835: Payment and remittance advice
- 811, 820: Premium payments
- 276, 277: Claim status
- 278: Referral certification and authorization

The **standard code sets** used under HIPAA are:

- International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM)[2]
- Healthcare Common Procedure Code Set (HCPCS) Level I codes (Current Procedure Terminology [CPT] codes)
- HCPCS Level II codes (medical and surgical supplies)
- Current Dental Terminology (CDT)
- National Drug Code (NDC)

The goal in developing one standardized methodology was to reduce the administrative cost of healthcare. This allows healthcare providers to use dollars previously spent on administrative costs to pay for the provision of healthcare.

HIPAA Privacy Rule

The HIPAA Privacy Rule states that "a covered entity may not use or disclose protected health information (PHI) except as permitted or required by this subpart or Subpart C of part 160 of this Subchapter."[3] This regulation is restrictive, meaning that using or disclosing PHI is not permitted unless an exception or requirement is satisfied. A covered entity is defined generally by the Privacy Rule as healthcare providers that transmit any health information in electronic form, a health plan with more than 50 participants, and a healthcare clearinghouse that receives, processes, and transmits health information for payment purposes.

Protected Health Information

The Privacy Rule defines PHI as individually identifiable health information that is created, collected, or stored by a covered entity and maintained in electronic or any other form (not including educational records). Individually identifiable health information is, generally, information that describes the past, present, or future health, condition, care, or treatment of an individual or payment for such care or treatment. In addition, individually identifiable health information must either identify the individual or contain a reasonable basis to

conclude that the information could be used to identify the individual. As such, the cumulative test to determine whether information could be deemed PHI includes the following three elements:

1. Health information that describes the past, present, or future health, condition, care, or treatment of an individual or payment for such care or treatment;
2. The information must reasonably identify the individual; and
3. The information must be maintained in electronic or any other form.

All three of these elements are required for the information to be considered PHI, which in turn triggers protection under HIPAA.

Deidentified Information

The HIPAA Privacy Rule excludes from its PHI definition any health information for which all the identifying characteristics listed in the regulations (approximately 18, depending upon how they are categorized) have been removed.[4] The presence of one of the 18 identifiers does not mean that the information is PHI. Rather, the *absence* of all 18 identifiers means, by rule, that the information does not reasonably identify the individual and is therefore not PHI. All 18 identifiers must be removed for health information to be considered deidentified.

Patient Privacy Rights

Keeping patient information confidential is not a new concept to healthcare providers. It has always been part of the ethical obligations of the physician-patient relationship. However, an overriding theme to the privacy regulations is to place control over health information squarely in the hands of the individual who is the subject of the information. Thus, in addition to regulating the uses and disclosures of PHI held by a covered entity, the Privacy Rule also provides individuals with certain rights regarding their PHI.

Individual Rights under the Privacy Rule

Federal privacy regulations under HIPAA grant individuals certain rights to be informed about and to control their PHI. These include the:

1. Right to access and obtain a copy of their PHI, including receiving electronic copies of all records in the designated record set
2. Right to amend their PHI
3. Right to obtain an accounting or listing of disclosures of their PHI
4. Right to receive a Notice of Privacy Practices
5. Right to have communications about their PHI conducted in a confidential manner
6. Right to restrict disclosure on certain uses and disclosures of their PHI
7. Right to file a complaint about a covered entity's privacy practices to the covered entity as well as to the Office for Civil Rights (OCR) of the U.S. Department of Health & Human Services

It is important that covered entities fully understand the exact nature of each right that HIPAA grants to individuals.

Right to Access PHI

The Privacy Rule requires that a covered entity provide individuals with access to their PHI or a copy of their PHI at their request. Individuals cannot necessarily have access to everything in the record. The covered entity can restrict the individual's access to such things as psychotherapy notes, information the covered entity compiled to prepare for actual or anticipated litigation, or PHI that the covered entity is prohibited from sharing pursuant to the Clinical Laboratory Improvements Amendments of 1988. A covered entity that is a correctional institution may also restrict an inmate's access to their PHI if the access would put the security of the individual, another inmate, or the institution at risk. Finally, the PHI can be restricted from an individual's access if the PHI was obtained during a research study and the individual agreed to the restricted access in the authorization signed at the beginning of the study; if the PHI was obtained from someone other than a healthcare provider and the individual was promised confidentiality; or if the PHI is subject to the federal Privacy Act.

A covered entity may also deny an individual access to PHI if a licensed healthcare professional has determined, based on their professional judgment, any of the following:

- Sharing the information would put the individual or another person in danger;
- The information was obtained from someone other than another healthcare provider and sharing the information would be reasonably likely to put that person at risk for substantial harm; or
- The request for access is from a personal representative and sharing the information would be reasonably likely to put the subject of the information or another person at substantial risk of harm.

If the individual is denied access for any of these three reasons, the covered entity is required to provide a method for the individual to appeal the denial. Another licensed healthcare professional must review the decision. The licensed healthcare professional reviewing the denial must not have been involved in the original decision to deny access. The covered entity is required to abide by the decision of the reviewing official.

The HITECH Act as finalized by the Omnibus Rule added the requirement that the covered entity must provide the PHI in an electronic format if the information is maintained electronically. Although no specific format is required, the covered entity is expected to work with the individual to determine a reasonable, acceptable electronic format for their records. A covered entity is permitted to send records through unencrypted emails provided, however, that "the individual was warned of and accepted the risks associated with the unsecure transmission."[5]

In early 2019, OCR announced the HIPAA Right of Access Initiative. The focus of the initiative was timeliness of access and related fees charged to access the information. Specifically, a covered entity should fulfill the request for access within 30 days of receiving the request. If the records cannot be obtained within that timeframe due to some difficulty, the covered entity may be afforded a single 30-day extension but must notify the individual in writing of the delay and provide the reason for the delay. In addition, covered entities are permitted to charge a reasonable fee for providing PHI to an individual, but the fee must only cover the cost to provide the record including labor, supplies, postage, and the time to complete a summary if required. In a press release on March 28, 2022, the OCR announced that a total of 27 enforcement actions have been resolved since the initiative began.[6]

Right to Request an Amendment to PHI

An individual may believe certain information in their health record is inaccurate or incomplete, and the individual has the right to request that the covered entity amend the information.

The covered entity may correct the record in a manner consistent with the entity's policies and procedures if the information is incorrect. Note that, as a general rule, original information documented in a medical record should not be altered in such a way as to completely eliminate the information.

A covered entity is not always required to make the requested amendment to the record. If the covered entity has determined that the record is accurate and complete, the individual's request for the amendment may be denied. The covered entity may also deny requests for other reasons. One reason is that the information was not generated by the covered entity. Another reason is that the individual wishes to amend information that the individual is not entitled to access or which is not part of the designated record set.

A covered entity has 60 days to act on the request for amendment. Even if the covered entity denies the request for amendment to the record, the covered entity must provide a response to the individual that includes the reason for the denial. In addition, the individual may submit a rebuttal to the denial and request that the rebuttal must be included as part of the individual's medical record.

Right to Request an Accounting of Disclosures

The HIPAA Privacy Rule gives individuals the right to know who has received their PHI. If an individual requests an accounting of disclosures, a covered entity must be prepared to provide the individual with a list of all disclosures it has made of the individual's PHI. An accounting is not required if the disclosure was:

- Used for treatment, payment, or healthcare operations
- Made as an incidental disclosure
- Made in a limited data set
- Made with an authorization from the individual
- Made for national security purposes
- Made prior to the enforcement date of the privacy regulations (April 14, 2003)
- Made to the subject of the information
- Required only giving the individual an opportunity to object
- Made to a correctional institution or other law enforcement official having custody of the individual for purposes of providing appropriate care to the individual[7]

The accounting must include who received the information, the date the disclosure was made, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. An individual may request an accounting that covers up to a six-year period.

HITECH added a requirement that healthcare providers that have implemented electronic health records are required to provide patients with an accounting of uses and disclosures for treatment, payment, and healthcare operations that are made from the electronic health record. The effective date depends on when the provider acquired their electronic record system. Final rulemaking has not been issued for this requirement and, as such, there is currently no requirement to include disclosures for treatment, payment, and healthcare operations in the accounting of disclosures.

Notice of Privacy Practices

Healthcare providers and health plans are required to provide patients with a copy of their notice of privacy practices that describes in easily understood terms how the covered entity is permitted to use and disclose an individual's PHI—and to provide examples of how patient health information will be used or disclosed. The notice also explains what the covered entity's legal obligations are under HIPAA, what the individuals' rights are, and who to contact with complaints and questions. For example, the notice must include a description of the types of uses and disclosures that require an authorization, a statement that other uses and disclosures not described in the notice will only be made with a written authorization from the individual, and a statement that the individual may revoke an authorization.

The notice should be carefully drafted. A covered entity is bound by the notice. Thus, if the notice does not fully describe how PHI is used and disclosed, it could be argued that the covered entity's ability to use and disclose information is more restrictive than what the privacy regulations allow. In addition, if the notice is revised, it must be made available upon request to an individual with whom the covered entity has a direct treatment relationship. For health plans, any material change to the notice requires prominent posting on its website of the change to the notice, or other provision to its covered individuals of the revised notice or information about the material changes. The Omnibus Rule required several changes to the Notice of Privacy Practices, thus constituting a revision or material change requiring redistribution and/or notification.

The notice must be provided to the individual at the first episode of care or as soon as reasonably practical after an emergency. The covered entity is required to make a good faith effort to obtain an acknowledgement from the individual that the notice of privacy practices was received. If the first episode of care was via the telephone, the covered entity must mail its notice to the individual within 24 hours. Calling the physician's office to schedule an appointment or calling the hospital to schedule a procedure would not be considered an episode of care.

Right to Request for Confidential Communications

Unlike restrictions which further limit the manner in which PHI can be used or disclosed, a request for a confidential communication addresses the manner in which PHI is communicated. If an individual makes a reasonable request to have PHI communicated in a specific manner, a healthcare provider is required to accommodate the request. What does this mean? An individual may ask that the provider only call one number to communicate PHI. The individual may ask that no messages are left on an answering machine or that messages are left only on the voicemail of the individual's cell phone. Unless the provider has a basis for arguing that the individual's request is unreasonable, an accommodation must be made to meet the request.

The confidential communication rule varies slightly for health plans. If a health plan receives a reasonable request for a confidential communication, accommodation of the request can be contingent on the individual stating that disclosure of the information in another manner could endanger the individual.

Right to Request Restrictions

An individual may request additional restrictions on the use and disclosure of PHI when it is for treatment, payment, or healthcare operations—or if the disclosure is made to a family member, friend, or another individual involved in the patient's care or payment for the care. These are the only further restrictions an individual is allowed to make for their PHI use and disclosure.

The Privacy Rule is very explicit. While an individual has the right to request a restriction, the covered entity is under no obligation to agree to the restriction. However, if a covered entity does agree to the additional

restriction on the use or disclosure of PHI, then the covered entity is bound by its agreement. An exception to the restriction rights was added and finalized with HITECH's Omnibus Rule, which requires that a healthcare provider not disclose health information about a particular health service to a health plan if three requirements are satisfied:

1. The individual requests that the information not be provided to the health plan;
2. The individual has paid out of pocket for the service in full; and
3. The health plan would normally obtain the information for payment or healthcare operations. This includes situations in which a family member is paying out of pocket for the service for the individual.[8]

Filing Complaints

The patient has a right to file a complaint regarding the covered entity's privacy practices with both the covered entity, usually to the privacy officer, as well as the OCR. The patient has the right to be notified of this and contact information is generally included in the notice of privacy practices.

Uses and Disclosures of Patient Information

The privacy regulations were drafted with the intent of allowing the free flow of information for the provision of healthcare and other purposes in the public interest. If a covered entity is not using or disclosing PHI for the direct provision of healthcare and related activities, then the method by which the information can be used, accessed, or disclosed will be limited.

A covered entity may only use or disclose PHI if the use or disclosure falls within one of the following five categories:

1. To carry out treatment, payment, or health care operations (TPO)
2. To the individual or to the HHS to investigate a privacy complaint
3. Pursuant to and in compliance with a valid authorization
4. When the individual must be given the opportunity to agree or object
5. An exception that does not require the individual's authorization or an opportunity to agree or object

Permitted Disclosures: TPO

PHI is used for one of three primary purposes: treatment, payment, and healthcare operations (TPO). If PHI use or disclosure fits into one of these three categories, it is not necessary to obtain explicit permission from the individual. This allowance ties directly to the intent of the privacy regulations to allow the free flow of PHI for purposes directly related to healthcare provision. Requiring an individual's permission to use or disclose PHI for TPO was deemed too cumbersome to allow for efficient and effective healthcare delivery.

Examples of TPO use or disclosure include:

- **Treatment**: A physician can call a colleague in another specialty to get the colleague's input on the care being provided.
- **Payment**: A physician's staff can submit a bill to the individual's insurance company to obtain payment for

the service provided.

- **Healthcare operations**: A physician's compliance staff can access the individual's PHI to conduct an assessment of the physician's coding and documentation practices.

Required Disclosures

Required disclosures are the second method through which a covered entity may use or disclose PHI without requiring permission from the individual. Only two instances exist under the Privacy Rule when the covered entity is required to disclose PHI:

1. When the information is requested by a secretary of HHS to investigate an allegation of a privacy violation; and
2. When the subject of the information requests it.

Please see "Right to Access PHI" for a discussion on the requirement to provide an individual with access to or a copy of their health information.

Authorizations

Uses and disclosures may only occur with permission from the individual in the form of an authorization. The authorization form must meet specific requirements including:

- Description of the PHI to be used or disclosed in a specific and meaningful fashion
- Name or other specific identification of the person or class of person(s) authorized to make the use or disclosure of the PHI
- Name or other specific identification of the person or class of person(s) authorized to receive the PHI
- Description of the purpose of each requested use or disclosure
- An expiration date
- Signature of the individual and date
- Statement informing the individual of the right to revoke the authorization in writing
- Any restrictions on the individual's right to revoke and instructions for how the authorization can be revoked
- Statement informing the individual that signing the authorization is a precondition of treatment, participation in research, eligibility for benefits, or enrollment in a health plan, if applicable
- Statement informing the individual that the recipient of the PHI may redisclose it in a manner that makes it no longer protected by the privacy regulations[9]

The individual is entitled to a copy of the authorization. If an authorization does not include all the required elements, it is invalid, and a covered entity cannot rely on it to use or disclose PHI. Marketing and fundraising are just two examples of uses and disclosures that require an authorization. As with any rule, however, there are exceptions. For a checklist of items needed for the authorization form, see Appendix 15. PHI Release

Authorization Checklist.

Access Requiring an Opportunity to Object

The next category of uses and disclosures requires covered entities to provide individuals with an opportunity to object prior to the use or disclosure occurring. Three purposes exist to which the opportunity to object applies and any one of the three purposes will allow access to the PHI.

The first purpose is when a covered entity includes limited information about the individual in its facility directory. An individual's name, location within the covered entity, general condition, and religious affiliation may be maintained in a directory. The information may be shared with members of the clergy. Other individuals inquiring about the individual by name can receive the person's name, location, and general condition. The subject of the PHI must be informed of the information that will be included in the directory and given an opportunity to object to the inclusion of all or some of the PHI in the directory. The individual must also be allowed to restrict to whom the directory information is disclosed. For example, an individual might not object to information being included in the directory but may not want it disclosed to a clergy member asking for information about individuals with certain religious affiliations.

A second disclosure can be made if the individual is given an opportunity to object. In this situation, a disclosure can be made to family, friends, or others involved in the individual's care or payment for the care. The information disclosed must be directly related to the individual's involvement in the subject's care. When the subject of the PHI is present, the disclosure can be made if the individual agrees to the disclosure, if the individual does not object to the disclosure, or if under the circumstances one can reasonably infer in the exercise of professional judgment that the individual does not object.

If the individual is not present or is incapacitated, a disclosure to family, friends, or others involved in the individual's care may be made if, in the exercise of professional judgment, the disclosure is in the best interest of the individual and the disclosure is limited to the PHI relevant to the party's involvement in the individual's care.

Finally, a covered entity can disclose PHI under this provision for purposes of assisting in disaster relief. The disclosure can be made to either a private or public entity authorized by law, or by its character, to assist with disaster relief. Such disclosures would generally be made so the location and condition of the individual could be accessible to family and friends.

Uses and Disclosures Not Requiring an Authorization or Opportunity to Object

A covered entity may use or disclose PHI without requiring permission from the individual if it falls under the general category of uses and disclosures deemed to be in the public interest. Most PHI uses and disclosures under these provisions carry restrictions on the circumstances for how and to whom the information can be used or disclosed. It is important to understand that the Privacy Rule permits, but does not require, the covered entity to use or disclose PHI for purposes in the public interest.

There are 12 categories under which a covered entity is permitted to disclose information in the public interest without first obtaining the individual's explicit permission. The categories include:

1. Required by law (different from the required disclosures discussed previously)
2. Public health activities
3. Reporting on victims of abuse, neglect, or domestic violence

4. Reporting for health oversight activities
5. Judicial or administrative proceedings
6. Law enforcement purposes
7. Information to coroners, medical examiners, and funeral directors about decedents
8. Information for organ donation
9. Certain research purposes
10. Disclosures to avert a serious threat to health or safety
11. Specialized governmental functions
12. Workers' compensation[10]

The details regarding circumstances when PHI can be used or disclosed for the listed public interest purposes are quite extensive. State law may also have a significant impact on uses and disclosures in the public interest. A discussion of these provisions with someone familiar with the particulars of the specific state or region where one practices is recommended.

Fundraising

If a covered entity wants to engage in fundraising, the HIPAA Privacy Rule permits the use of limited PHI without an authorization. The limited PHI includes demographic information such as name, address, or other contact information; insurance status; and date of care. This information can be used for fundraising activities by the covered entity or disclosed to the covered entity's business associate or institutionally related foundation. If the covered entity wants to use additional PHI, an authorization from the individual would be required.

HITECH, finalized by the Omnibus Rule, added the requirement that all fundraising communications provide the individual with a clear and conspicuous way to opt out of receiving further fundraising requests. The method to opt out must be easy for the individual to understand and use and should cost no more than a nominal amount, such as the price of a postage stamp. Once an individual has opted out, the covered entity is prohibited from sending further fundraising communications to the individual. The covered entity is also prohibited from conditioning treatment or payment on the individual's choice to opt out.

Marketing of PHI

The Privacy Rule prohibits the use of PHI for marketing purposes unless the patient specifically authorizes the disclosure of the information and was notified by the provider that it received direct or indirect remuneration for the disclosure.

If the marketing activity is a face-to-face encounter with the individual, or if an item of nominal value is given to the individual, an authorization is not required. It is helpful to note that the definition of "marketing" under HIPAA does not include information given to an individual about particular benefits or services that are part of the individual's health plan, such as information related to the individual's treatment, alternative treatments, therapies, healthcare providers, or settings of care.

HITECH, finalized by Omnibus Rule, further restricts the use of PHI for marketing activities and expands the requirement for an authorization for certain health-related communications sent by a healthcare provider to an

individual in exchange for financial remuneration received from the third party whose product or service is being described. For example, an authorization is required when a healthcare provider sends out a notice about new state-of-the-art medical equipment if the equipment manufacturer paid the costs of sending the mailing to the patients. There is a limited exception for refill reminders.

For subsidized treatment communications, healthcare providers are required to disclose within the authorization that remuneration was received and provide an opportunity for the patient to opt out of receiving such communications.

HIPAA Privacy Rule: Other Issues

In addition to understanding general requirements for uses and disclosures permitted by HIPAA, certain overarching principles are equally important components of the privacy regulations. The components include:

1. Minimum necessary standards
2. Verification requirements prior to releasing PHI
3. Disclosures to business associates
4. Breach notification requirements

Minimum Necessary Standards

The term "minimum necessary" is used in HIPAA to identify the amount of PHI that can be used or disclosed in a particular circumstance. For most PHI uses and disclosures, the regulation requires that the covered entity only share the minimum amount needed to accomplish the task or activity. Virtually any time a covered entity makes a use or disclosure, an evaluation of minimum necessary will be required, however there are certain circumstances under which a minimum necessary evaluation is not required. These circumstances include uses or disclosures made:

- With an authorization
- To a provider for treatment
- To the subject of the information
- To the HHS Secretary
- As required by law
- As required to comply with the regulations[11]

What constitutes the minimum amount necessary will be based on the situation. In some cases, the minimum necessary amount of PHI may include the entire record. However, an assessment of minimum necessary is still required. If a covered entity makes routine uses or disclosures for particular purposes, a policy and procedure can be written to define minimum necessary. Having a policy will eliminate the need to individually assess each use or disclosure.

Minimum necessary also ties to two additional concepts: role-based access and need-to-know. Role-based access means only allowing employees and others access to the information that is needed to perform their role in the organization. For example, a nurse in the ICU may need a different level of access than a dietician would

need.

The second concept—need-to-know access—is generally an educational process. In some instances, a covered entity grants an individual full access to the medical record because it is appropriate, based on the individual's role. However, it is unlikely the individual will have a business need-to-know for all information the individual has the ability to access. For example, a physician or resident may be granted access to the entire electronic health record of a covered entity. If the physician does not have a treatment relationship with a particular patient, it would not be appropriate for the physician to look at the individual's record. Stated another way, the ability to access PHI does not equate to a "need-to-know" the information.

Covered entities must determine the appropriate level of access to be granted to various individuals based on their roles. The next step is to educate those individuals who have access regarding the proper PHI uses and disclosures.

Verification Requirements Prior to Releasing PHI

When PHI is requested from a covered entity, how does the covered entity know that the requesting party is legitimately entitled to the requested PHI? There is no definitive answer to this question. However, the privacy regulations do require the covered entity to have in place reasonable methods to verify the individual's identity and that person's right to receive the information.

For example: If a physician calls a hospital requesting lab results, the hospital staff could ask a few questions to verify the physician has a treatment relationship to the individual whose information is being requested. The physician might be asked for date of birth (DOB), medical record number (MRN), the reason for the lab test, or some other piece of information.

There is no magic formula that can determine what is reasonable. What is most important is that a covered entity has a process for verification, a rationale for why the process is reasonable, and evidence that the process is consistently followed.

Disclosures to Business Associates

Often a covered entity contracts with an external company or individual to provide services that would typically be performed by the covered entity. If the service performed by the outside entity on behalf of the covered entity includes the use or disclosure of PHI, the outside entity is called a business associate (BA). Common types of services constituting a BA relationship include accounting, outside legal counsel, coding and billing services, transcription services, and vendors of electronic health records (if the vendor has access to electronic PHI). HITECH also includes in its BA definition vendors of personal health record systems and patient safety organizations.

Before PHI can be shared between a covered entity and a BA, there must be a Business Associate Agreement (BAA) in place. The BAA sets forth the PHI that will be used by BA, how the PHI will be used, the safeguards for protecting the PHI, the return or destruction of the PHI at the conclusion of the agreement, and other similar protections. Assuring that a proper BAA is executed is a requirement under the HIPAA Privacy Rule.

HITECH extended compliance requirements for covered entities to BAs. In addition to complying with the Privacy Rule, BAs are required to comply with the technical, administrative, and physical safeguard requirements under the Security Rule. In addition, BAs are accountable to HHS and directly liable for criminal and civil penalties for uses or disclosures that violate the Privacy and Security rules. This applies to BAs whether or not they have an agreement in place with the covered entity.

The Omnibus Rule further extended BA requirements to subcontractors of BAs. As a result, BA subcontractors are required to have a privacy and security program and are directly liable for criminal and civil penalties for uses or disclosures in violation of the Privacy Rule. Even though the Omnibus Rule extends the liability for privacy violations to subcontractors of a BA, the covered entity is ultimately responsible for the actions of its BAs or subcontractors of the BA in the event of a reportable breach of PHI.

Breach Notification Requirements

Since implementing HIPAA's Privacy and Security rules, healthcare providers and health plans have had significant breaches of patient information, including those due to having unencrypted PHI on lost or stolen laptops and other types of computer devices. The risk to patients includes breaches of confidential information and the potential for identity theft if the information contains identifiers such as Social Security numbers, health plan account number, or other similar identifiers.

Information Security Risk Identification and Safeguards

Technological advances have yielded significant benefits for many organizations, not the least of which was enabling a remote workforce. However, as organizations have become more dependent upon technology, the risk of a breach of PHI and confidential or financial information has also increased. Even large organizations or ones with mature information security programs are at risk. According to data published by Crowdstrike in its 2022 *Global Threat Report*, ransomware-related data leaks in 2021 increased by 82%. Campaigns to intrude into networks increased by 45%, and 21 new cyber adversaries were identified and named, bringing the total number of tracked adversaries up to more than 170.[12] Adversaries continued to adapt their technology to ever-changing operational opportunities and world events.

Even with robust security programs, protecting PHI is often a people-driven exercise. For example, an organization may have in place a robust information security program, but one employee who follows a link that prompts for a system username and password could expose the entire network. Imagine you have the most secure vault in the world, but access to that vault could be gained with one key. If the person holding that key is careless or tricked, the vault is accessed and the contents of the vault are breached. Therefore, it is not enough to invest in the information security infrastructure. Additional investment must be made in the people who have access to the information security infrastructure to limit the exposure to the PHI maintained by the organization.

The problem of cyberattacks has only been exacerbated with the expansion of the remote workforce. Phishing, spear phishing, smishing, and other attempted attacks are becoming more and more convincing by misappropriating business logos, email addresses, and other messages that on the surface appear to be legitimate. Moreover, not all safeguards may be available on all platforms. For example, when a user receives a suspicious email on a laptop, placing the cursor over the email address will reveal the full address of the sender, which can provide insight about whether the sender is legitimate. Similarly, hovering over a link within an email, when viewed on a computer, will reveal the URL of the link, which can indicate whether the link is

legitimate. However, neither of those safeguards is available for the person who views the same email on a smartphone if it has not been properly configured. As a result, a seemingly benign message from the office platform stating that a routine password change is required and can be completed by following the link can result in an unauthorized access to the organization's secured network. For that reason, even if the organization has a highly sophisticated information security program, it is crucial that the organization invest in education and practice for their employees to help stop network intrusions.

A breach is a violation of the HIPAA Privacy Rule. Several exceptions to what constitutes a breach have been defined in the Privacy Rule, including:

- Disclosures where there is a good faith belief that the recipient of the information would not reasonably have been able to retain the information;
- Certain unintentional acquisition, access, or use of the information by persons or employees acting under the authority of the covered entity or BA; or
- Certain inadvertent disclosures among persons similarly authorized to access PHI of a BA or covered entity[13]

HITECH created an obligation on the part of covered entities and their BAs to notify individuals of the breach in the event that it meets the reportable breach standard. A reportable breach occurs when there is a violation of the HIPAA Privacy Rule of unsecured PHI. The Omnibus Rule modified the standard for a reportable breach so that it is presumptively reportable if there is a violation of the Privacy Rule and the information was unsecured. "Presumptively reportable" means that the covered entity must report any breach of unsecured PHI unless it determines there is a low probability of compromise of the PHI. The determination of "compromise" is made by the organization after assessing the level of harm that has, or could reasonably occur, to the individual whose PHI has been breached.

The Omnibus Rule established that the assessment of whether there is a low probability of compromise is based on four factors: (1) content, (2) person, (3) access, and (4) mitigation. There is no uniform methodology for completing this assessment. Instead, the covered entity must be able to present supporting documentation to evidence its reasonable belief that the breached information had a low probability of compromise to the individual based on the four factors.

HHS issued guidance regarding securing health information and specifically the technologies and methodologies that would make PHI unusable, unreadable, and indecipherable. For electronic information, the National Institute of Standards and Technology (NIST) published the resource guide, "Implementing the Health Insurance Portability and Accountability Act Security Rule: A Cybersecurity Resource Guide" in July 2022. This document provides guidance and a framework to assist covered entities in protecting ePHI and to better understand the concepts in the HIPAA Security Rule.[14] For PHI in nonelectronic formats, methodologies include deidentifying the information; or shredding, pulping, or otherwise treating the material so the information cannot be reconstructed.

Once a breach is determined to be reportable, the covered entity is required to provide notification to the individual or their representative, as well as the OCR. For individuals who are deceased, the notice must be provided to their next of kin. If the covered entity does not have sufficient addresses for the individuals, or if some notices are returned undeliverable, the covered entity must provide a substitute notice as soon as possible,

such as by phone or email. If 10 or more breach notifications are returned undeliverable, then the covered entity must post information about the breach in a conspicuous place on the home page of its website along with a toll-free number for individuals to obtain information about the breach.

Reportable breaches involving 500 or more individuals must be reported immediately to HHS via an online reporting system on the OCR website.[15] The covered entity must also notify the individuals whose information was violated, as soon as possible but no later than 60 days after the breach occurred. When the reportable breach involves more than 500 individuals in a single state or jurisdiction, media outlets in the areas where patients reside must also be notified (e.g., radio and television stations), with a notice that includes the same information about the breach that is provided to the affected individuals.

For reportable breaches involving fewer than 500 individuals, the covered entity must report the breaches in an annual disclosure to HHS within 60 days of the end of the prior calendar year through the same online reporting mechanism.

The notice to the individual must include:

- A description of what happened, including the date of the breach and the date of the discovery
- Description of the types of information involved in the breach
- Steps individuals can take to protect themselves from harm
- Description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and protect against further breaches
- Contact information for individuals to ask questions or learn additional information, which must include a toll-free number, an email address, website, or postal address[16]

Enforcement and Penalties

Enforcement of the Privacy Rule is the responsibility of the OCR and was initially a complaint-driven process. Over time, enforcement efforts have increased along with civil monetary penalty (CMP) increases that can be applied to covered entities for violations of the rules and breaches of PHI. HITECH added tiers of penalty amounts and set a minimum and maximum penalty for each level of a violation. Under HITECH, the penalty for violations was set at $100 at the lowest level and up to $50,000 per violation at the highest level. The calendar year cap for any identical violation was raised from $25,000 under HIPAA to $1.5 million under HITECH.[17] The Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 provided authority to HHS to make annual adjustments to the amounts of CMPs. On March 17, 2022, HHS published the adjusted CMP amounts for 2022. The 2022 minimum CMP is $127, with a maximum of $63,973. The calendar year cap for any single violation is $1,919,173.[18] The penalties for violations are loosely based on a four-tier system that considers whether the breach was accidental or intentional, as well as the actions that the covered entity undertook to correct the breach and prevent future breaches.

The four tiers, along with the adjusted penalty amounts, are as follows:

- Violations in which there was an inadvertent violation, and the covered entity would have taken different action if they were aware of the violation, with a penalty for each violation of a minimum of $127 up to $63,973.[19]

- Violations due to reasonable cause but not willful neglect with penalties from a minimum of $1,280 for each violation to a maximum of $63,973.[20]
- Violations due to willful neglect but the problem was corrected by the covered entity. Fines range from a minimum of $12,794 per violation to a maximum of $63,973.[21]
- Violations due to willful neglect and uncorrected problems start at a minimum of $63,973 and can reach $1,919,173.[22]